Alerte d'attaque par phishing sur ZIMBRA

Un mail provenant de « **adquisiciones@fadu.edu.uy** » est envoyé aux utilisateurs de Zimbra leur notifiant l'expiration de leur mot de passe. Il leur est ensuite demandé de changer le mot de passe Zimbra avec l'option de garder le même mot de passe en le redirigeant vers une page de connexion.

Le but de cette campagne est de récupérer les comptes d'accès et les mots de passe des utilisateurs de Zimbra.

Ces données récupérées peuvent être utilisées pour accéder non seulement aux mails professionnels mais aussi à d'autres comptes des victimes (réseaux sociaux, banque en ligne, autres adresses emails) sachant que les utilisateurs dans la plupart des cas réutilisent le même mot de passe pour différents services.

Voici le lien en question :

- *hxxps://tfb.intrabench.com/?redirect&__CONFIRM=11111.myZOJSzidI.383&REDIRECT=T&__URL=http://gouv.tg.2EbT.d3rpsqu4d[.]net/a?Y2luYS5sYXdzb25AZ291di50Zw==*

[Attention, ne pas cliquez sur le lien]

Conseil N°1 : NE PAS cliquer sur le lien.

Conseil N°2 : Au cas où vous auriez cliqué sur le lien

- **Appeler CERT.tg sur le 22-53-59-80 ou déclarer l'incident sur www.cert.tg**
- **Changer tous vos mots de passe sur tous vos comptes**
- Il est recommandé d'**utiliser des mots de passe différents pour chaque type de compte**

Conseil N°3 : Un outil de gestion de mots de passe peut être utilisé pour la gestion de vos mots de passe

Conseil N°4 : Pour les administrateurs

- **S'assurer de la non présence des indicateurs de compromission (IOC)**
- **En cas de présence des IOCs, il faudra s'assurer que les recommandations sont effectivement mises en œuvre**
- **Sensibiliser les utilisateurs sur les bonnes pratiques**

Indicateurs de compromission :

- *adquisiciones@fadu.edu.uy*
- *gouv.tg.2ebt.d3rpsqu4d[.]net*
- *d3rpsqu4d[.]net*
- *hxxps://tfb.intrabench.com/?redirect&__CONFIRM=11111.myZOJSzidI.383&REDIRECT=T&_URL=http://gouv.tg.2EbT.d3rpsqu4d[.]net/a?Y2luYS5sYXdzb25AZ291di50Zw==*
- *IP : 162.241.124.47*